Scott A. Kamber (*pro hac vice*)
skamber@kamberlaw.com
David A. Stampley (*pro hac vice*)
dstampley@kamberlaw.com
KamberLaw, LLC
100 Wall Street, 23rd Floor
New York, New York 10005
Telephone: (212) 920-3072
Facsimile: (212) 202-6364
Interim Class Counsel

UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF CALIFORNIA
SAN JOSE DIVISION

IN RE IPHONE APPLICATION LITIG.	CASE NO. 11-MD-2250-LHK The Honorable Lucy H. Koh **DECLARATION OF LODOVICO MARZIALE IN SUPPORT OF PLAINTIFFS' OPPOSITION TO DEFENDANT APPLE INC.'S MOTION FOR SUMMARY JUDGMENT**

CONTENTS

I, Lodovico Marziale, declare as follows:

1. I am Co-Founder of 504ENSICS, LLC. I submit this declaration in support of Plaintiffs' opposition to Defendant Apple Inc.'s motion for summary judgment in this case. I am familiar with and have personal knowledge of the matters set forth in this declaration and if called upon to do so, could and would testify competently thereto, except where my knowledge is based upon information and belief, and as to those matters, I understand and believe them to be true.

I. OVERVIEW OF OPINIONS

2. I have been asked to state my opinion regarding the following matters:

(a) Using dynamic analysis, determine what, if any, Subject information is transmitted, and to whom, by each of five specific iPhone apps: Dictionary.com, Flixster, Pandora, Urbanspoon, and The Weather Channel.

(b) Using dynamic analysis, determine what, if any, location data is sent from Apple's iPhone, specifically when location services have been turned off.

II. QUALIFICATIONS

3. I am Co-Founder of 504ENSICS, LLC, a research and development firm that specializes in the fields of digital forensics and computer security. Additionally, 504ENSICS offers network vulnerability assessment, penetration testing, digital forensics and data recovery services, and training. My responsibilities include performing each of the previously listed services as needed.

4. My highest degree obtained is a Ph.D. in Engineering and Applied Sciences (Major: Computer Science) from the University of New Orleans.

5. I have published numerous peer-reviewed works in books, journals, and conference proceedings.

6. I have given talks on topics in digital forensics at several conferences including DOD Cybercrime, the Digital Forensics Research Conference (DFRWS), and the Open Source Digital Forensics Conference. I have conducted workshops on digital forensics at conferences.

7. I have taught courses at the undergraduate and graduate level in computer security and cryptography at the University of New Orleans.

8. I am Co-Developer of two widely used open source tools for digital forensics: the Scalpel file carver, a data recovery tool; and Registry Decoder, a tool for analysis of the Windows registry.

9. I am currently working on and have co-written two funded grant proposals for the DARPA Cyber Fast Track Program. The first, "Application-Level Memory Forensics for DALVIK," focuses on memory forensics on Android devices including mobile handsets. The second, "Forensic Analysis of the OS X Spotlight Search Index," focuses on reverse engineering the Apple OS X Spotlight disk indexing facility for forensics.

10. I have extensive knowledge of network protocols and traffic analysis as a result of my teaching duties as well as performing network security audits.

11. I am a GIAC Certified Forensic Analyst (GCFA).

12. Additional qualifications are listed in my curriculum vitae attached as Exhibit 1, which also includes a list of all publications I have authored in the previous ten years and a list of all other cases in which, during the previous four years, I have testified as an expert at trial or by deposition.

III. METHODOLOGY

A. Acquisition

13. I was provided three iPhones for testing. The first was a phone provided to me by KamberLaw (TEST) on or about 12/26/2012. The second iPhone was reportedly owned by Anthony Chiu (CHIU) and the third was reportedly owned by Cameron Dwyer (DWYER). The CHIU and DWYER phones were provided by Milberg on 01/14/2013. The UDIDs specified for CHIU and DWYER are as provided by KamberLaw. The UDID for TEST was provided by manual inspection in iTunes. Model and OS of each iPhone was provided by manual inspection.

Phone	Serial	UDID	Model	OS
CHIU	[redacted]WA4T	[redacted]5fc1	4	5.1
DWYER	[redacted]7EDG	[redacted]892c	3GS	5.1.1
TEST	[redacted]KEDG	[redacted]d214	3GS	4.1

Table 1: iPhones

B. Setup

11. I began by configuring a testing workstation to act as a web traffic proxy and intercept and record all web traffic directed to the proxy. In order to accomplish this I installed and configured the Fiddler Web Debugger (v2.4.2.4), a widely used application for web traffic analysis.

12. Prior to testing, each iPhone was configured to use its WiFi connection and to connect to my local wireless network. I then set each iPhone to use the Fiddler proxy on the testing workstation for all web traffic. This arrangement caused web traffic leaving and returning to the iPhone was intercepted and recorded by the Fiddler application.

13. Except where noted otherwise, all three iPhones had Location Services turned on.

C. Testing

14. I tested the following five applications: The Weather Channel, Urbanspoon, Flixster, Dictionary.com, and Pandora. Only Flixster and Pandora were available for analysis on the DWYER iPhone. All five apps were available on the remaining two iPhones. The versions of the applications as tested are listed below.

App	TEST	CHIU	DWYER
Dictionary.com	3.0 December 20, 2010	3.0 December 20, 2010	NA
Flixster	5.4.1 May 30, 2012	5.30 Apr. 19, 2012	5.20 Feb. 21, 2012

Pandora	3.1.13 July 27, 2011	3.1.22 Mar. 17, 2012	3.1.20 Feb. 7, 2012
Urbanspoon	1.17 Dec. 20, 2010	2.0.2.1 ~Apr. 20, 2012	NA
The Weather Channel	4.1.1 r172755 Oct. 15, 2011	4.3.0 r 182925 Mar. 24, 2012	NA

Table 2: App Versions (Dates from iTunes App Store)

15. In testing each of the three iPhones, I followed the same sequence of steps:

(a) On the testing workstation, set Fiddler to begin capturing web traffic.

(b) Open the app to test.

(c) Wait 5-10 seconds for the app to finish loading.

(d) Note the session number in the Fiddler. Subject data from web traffic up to this session number is noted in the spreadsheet attached as Exhibit 3 in the "When" column as "On Start."

(e) Perform an action with the app (e.g., search).

(f) Wait 5-10 seconds for the action to complete.

(g) Note the session number in the Fiddler. Subject data from web traffic up to this session number is noted in the spreadsheet attached as Exhibit 3 in the "When" column as "<action>"

(h) Close the application.

(i) Save the web traffic recorded by Fiddler.

(j) Reset Fiddler.

(k) Continue to the next application.

16. I then performed a second round of testing specifically focused on location data transmitted to Apple-controlled servers when location services were turned off. I performed the following sequence of steps on the TEST iPhone:

(a) Turn off location services.

(b) On the testing workstation, set Fiddler to begin capturing web traffic.

(c) For each of the five apps being tested, open the app.

(d) Wait a 5-10 seconds for the app to finish loading.

(e) Perform an action with the app (e.g., search).

(f) Wait 5-10 seconds for the action to complete.

(g) Close the app.

(h) After running all five apps, save the web traffic recorded by Fiddler.

(i) Examine the recorded web traffic and determine if location data was sent to Apple-controlled servers. Record this location data as "Location Off" in the spreadsheet attached as Exhibit 3.

IV. Analysis Notes

17. I analyzed the web traffic recorded by Fiddler, also using the Fiddler application as my analysis platform. My analysis involved manually searching for Subject data in the recorded web traffic. The table attached as Exhibit 2 summarizes my findings.

18. I have determined that significant amounts of Subject information are sent by the above listed applications to remote servers controlled by those apps' companies. A non-exhaustive list of Subject information is shown in Exhibit 2.

19. Further, I have determined that significant amounts of Subject information are sent by the above listed applications to remote servers controlled by several other third party entities such as shown in Exhibit 2.

20. I have also determined that the iPhone does transmit location data, including the BSSID of nearby wireless access points to remote servers controlled by Apple when location services are turned off.

21. There were many strings of the form "iPhone 3,1" and similar. These appear to be internal Apple names which map directly to handset model and OS version as provided here[1].

22. At least 2 sessions in the spreadsheet attached as Exhibit 3 contained numbers which appeared to be wireless access point BSSIDs. I then used the inSSIDer (v2.1.6.1395) wireless network scanner to verify that the BSSIDs seen were in fact wireless access points near my location at the time of testing.

23. At least 2 sessions involving "Medialytics" in the spreadsheet attached as Exhibit 3 had a named field in the GET request string which labeled "UDID." The related value however was not the UDID for the iPhone being tested. This value is consistent with the UDID-derived identifier in this source[2] that cannot be reversed. This value also appeared to be a 16 byte hexadecimal-encoded number which would be consistent with an MD5 hash of data containing the UDID in some permutation.

24. The column "Other Data" in the spreadsheet attached as Exhibit 3 contains both cookie data and POST data. Selected POST data was provided that appeared as human readable content.

V. OTHER

25. My opinions in this declaration are based on my extensive experience as a digital forensics and computer security researcher and practitioner.

26. Documents and resources I considered in formulating the opinions set out in this declaration are as noted above.

27. My compensation to be paid for my study and testimony in this case is US$ 250 for consultation and US$ 350 for testimony.

[1] http://theiphonewiki.com/wiki/Models

[2] http://www.medialets.com/medialets-universal-sdk-2-6-3-for-ios-released/

I declare under penalty of perjury under the laws of the United States of America that the foregoing is true and correct.

Executed on January 22, 2013 at Orleans Parish, Louisiana.

LODOVICO MARZIALE